REMARKS

Claims 11, 14-15, 17, 20-21, and 23 are pending and under consideration.

Favorable reconsideration of this application, in light of the following discussion, is respectfully requested.

I. Objection to the Specification

In the Office Action, the specification was objected to as failing to provide proper antecedent basis for the claimed subject matter.

This objection is respectfully traversed.

More specifically, the Examiner has objected to the claim limitation "a public switched telephone network that is distinct from the packet-oriented data network." The Examiner appears to take the position that this feature is not supported in the specification because it is disclosed that the public switched telephone network can be an ISDN. However, this is irrelevant to whether or not the claimed public switched telephone network is distinct from the claimed packet-oriented data network. In other words, just because the public switched telephone network can be an ISDN, it does not follow that the disclosure does not support the position that there are two distinct networks, one being a public switched telephone network and the other being a packet-oriented data network. Fig. 1 of the drawings and the corresponding disclosure clearly indicate that there is both an IP-based LAN and a separate and distinct public TDM telephone network. For example, paragraph [0015] of the specification clearly states "the heterogeneous network shown in Figure 1 on the one hand includes an IP-based LAN (LAN = Local Area Network) **as well as** a public TDM (TDM = Time Division Multiplexing) telephone network."

Accordingly, withdrawal of the objection is respectfully requested.

II. Rejections under 35 U.S.C. § 112

In the Office Action, claims 11, 14-15, 17, 20-21, and 23 were rejected under the first paragraph of 35 USC § 112 as failing to comply with the written description requirement.

In the Office Action, claims 11, 14-15, 17, 20-21, and 23 were rejected under the second paragraph of 35 USC § 112 as being indefinite.

These rejections are respectfully traversed. For the reasons discussed above with respect to the objection to the specification, it is submitted that claims 11, 14-15, 17, 20-21, and

23 do comply with the written description requirement and are definite with respect to the claimed feature of "a public switched telephone network that is distinct from the packet-oriented data network."

Accordingly, withdrawal of the § 112 rejections is respectfully requested.

III. Rejection under 35 U.S.C. § 103

Claims 11, 14-15, 17, 20-21, and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0009659 to DiSanto et al. (hereinafter "DiSanto") in view of the article "*Conversational IP multimedia Security*" by Blom et al. ("Blom").

Independent claim 11 recites:

> A security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network, and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway, said security module being connected into a connecting line of one of the first and second telecommunication terminals and comprising
>
> a protocol processing unit processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals;
>
> a modem connection unit, used when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of a gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection, wherein
>
> a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol, and
>
> the encrypted transport protocol is Secure Real Time Transport

Protocol.

As such, claim 11 provides a protocol processing unit that processes data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol. Furthermore, claim 11 includes a modem connection unit, used when the security module is connected in a connecting line at a second telecommunication terminal, that transports the data packets using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. As such, the security module of claim 11 provides for end-to-end encryption between a client in a packet-oriented network and a client in a public switched telephone network (analog or digital), which is distinct from the packet-oriented network, using the key exchange protocol and the encrypted transport protocol (SRTP) because each of the two distinct networks distinctly use the key exchange protocol and the encrypted transport protocol via the claimed protocol processing unit and modem connection unit, respectively. These features are not taught by either DiSanto or Blom.

The Examiner's statement that applicant is arguing that the claimed networks "use" the recited key exchange protocol and the encrypted transport protocol is not correct. As clearly stated, applicant is asserting that each of the recited key exchange protocol and the encrypted transport protocol are provided via the claimed protocol processing unit and modem connection unit, which are part of the claimed security module.

Furthermore, the modem of DiSanto does not correspond to the claimed modem connection unit, as indicated by the Examiner. As discussed above, the claimed modem connection unit when the security module is connected in a connecting line at a second PSTN telecommunication terminal for transporting the data packets using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. As such, the claimed modem connection unit provides a transfer of encrypted communications from the packet-oriented network into the PSTN because the packet-oriented network also uses the encrypted transport protocol with keys for the encrypted transport protocol exchanged using the key exchange protocol.

DiSanto merely discloses a security device for secure communication over a plurality of networks (see DiSanto's Abstract). The internal modem 240 in FIG. 2B of DiSanto is used to perform analog to digital conversion when digitized voice data is directed to port 245 (see paragraph [0033] of DiSanto). Thus, the modem 240 is used merely to comply with the technical requirements of a respective network, but does not provide a technical solution enabling encryption of voice data in a heterogeneous network including a packet-oriented network and a

PSTN. Again, DiSanto does not disclose a heterogeneous network including a separate and distinct packet-oriented network and PSTN. Thus, it follows that the internal modem 240 of DiSanto cannot perform the function as providing a path for encrypted communication as stated by the Examiner and as recited in independent claim 11.

Furthermore, claim 11 specifies that "a point-to-point protocol connection is used over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol." The Examiner alleges that this feature is anticipated by "a procedure for establishing a direct connection between two nodes" disclosed in DiSanto. However, unlike in DiSanto, the modem of the claimed security module enables the data packets from the packet-oriented network to be transported using the encrypted transport protocol, along with messages of the key exchange protocol, via the modem connection. The procedure for establishing a direct connection between two nodes in DiSanto does not anticipate or render obvious this type of connection among terminals of different networks.

At least for the above reasons, claim 11 and pending claims 14-15, 17, and 20-21 depending from claim 11 patentably distinguish over the prior art.

Claim 23 recites:

> A method performed by a security module for encrypting a telephone conversation between at least one first telecommunication terminal using a Voice over IP (VoIP) system in a packet-oriented data network and at least one second telecommunication terminal in a public switched telephone network that is distinct from the packet-oriented data network and that is at least one of analog and digital and is connected to the packet-oriented network via a gateway, said security module being connected into a connecting line of one of the first and second telecommunication terminals and comprising
>
> processing data packets transported on the packet-oriented network using the encrypted transport protocol with keys for the encrypted transport protocol exchanged using a key exchange protocol, converting voice signals, created by the one of the first and second telecommunication terminals at which said security module is connected, into data packets for transport via the encrypted transport protocol and converting data packets, arriving at said security module after transport via the encrypted transport protocol, into voice signals;
>
> when said security module is connected in a connecting line at a second telecommunication terminal, setting up a modem connection between the second telecommunication terminal and at least one of the gateway and another second telecommunication terminal, with the data packets being transported using the encrypted transport protocol, along with

messages of the key exchange protocol, via the modem connection; and

using a point-to-point protocol connection over the modem connection in transporting the data packets using the encrypted transport protocol, as well as messages of the key exchange protocol, wherein

the encrypted transport protocol is Secure Real Time Transport Protocol.

For at least the reasons discussed above with respect to claim 11, it is respectfully submitted that the cited prior art does not teach each of the features of claim 23, so that claim 23 patentably distinguishes over the prior art.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 3-7-11

By: _____

Aaron C. Walker
Registration No. 59,921

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501